

WHAT IS CLAIMED IS:

1. In a data processing system, a method comprising the steps of:  
creating a migratable storage tree with a storage root key; and  
creating a non-migratable storage tree with the storage root key, wherein the  
migratable storage tree and the non-migratable storage tree are identically structured.
2. The method as recited in claim 1, wherein the migratable storage tree and the  
non-migratable storage tree are created by a trusted computing module in accordance  
with Trusted Computing Platform Alliance.
3. The method as recited in claim 1, wherein the migratable storage tree  
comprises migratable keys and a user key, wherein the non-migratable storage tree  
comprises non-migratable keys and a user key.
4. The method as recited in claim 1, wherein the non-migratable storage tree will  
include non-migratable storage keys corresponding to each migratable storage key in  
the migratable storage tree.
5. The method as recited in claim 1, wherein use authorization in the  
non-migratable storage tree will be identical to use authorization in the migratable  
storage tree.

1 6. The method as recited in claim 1, further comprising the steps of:  
2 requesting a migratable storage key; and  
3 requesting a non-migratable storage key.

1 7. The method as recited in claim 6, wherein the step of requesting a migratable  
2 storage key will identify a parent key in the migratable storage tree, and wherein the  
3 step of requesting a non-migratable storage key will identify a parent key in the  
4 non-migratable storage tree that corresponds to the parent key in the migratable  
5 storage tree.

1 8. The method as recited in claim 1, further comprising the step of:  
2 when a key loading request is made for a migratable storage key, loading a key  
3 from the non-migratable storage tree instead of loading a corresponding key from the  
4 migratable storage tree.

1 9. In a data processing system, a method comprising the steps of:  
2 splitting a request to create a new migratable storage  
3 key with given authentication data and a first parent key into first and second  
4 commands;  
5 wherein the first command creates a migratable storage key with the given  
6 authentication data and the first parent key; and  
7 wherein the second command requests creating a non-migratable storage key  
8 with the given authentication data and a second parent key which is determined from  
9 looking up a key that corresponds to the first parent key in a database.

1 10. The method recited in claim 9, wherein the migratable storage key and the  
2 non-migratable storage key are associated in a database.

1 11. The method recited in claim 9, wherein the non-migratable key is a multi-  
2 prime key.

1 12. The method recited in claim 9, where the non-migratable key is an elliptic  
2 curve key.

1 13. The method as recited in claim 9, further comprising the steps of:  
2 creating a new migratable signing key with the given authentication data and a  
3 third parent key;  
4 storing the new migratable signing key with the given authentication data and  
5 the third parent key;  
6 storing the new migratable signing key with the given authentication data and  
7 a fourth parent key where the fourth parent key is a non-migratable key associated  
8 with the third parent key in a database.

1 14. The method as recited in claim 13, further comprising the steps of:  
2 requesting a signature by the new migratable signing key;  
3 searching the database for the location of a key blob containing the new  
4 migratable signing key;  
5 loading a copy of the new migratable signing key stored in the key blob  
6 created with the non-migratable parent key; and  
7 signing with the new migratable signing key.

1 15. The method as recited in claim 9, further comprising the steps of:  
2 creating a new data stored by means of the first parent key;  
3 storing the new data with the first parent key;  
4 storing the new data with the second parent key where the second parent key is  
5 a non-migratable key associated with the third parent key in a database.

1 16. The method as recited in claim 15, further comprising the steps of:  
2 requesting data stored by the new migratable storage key;  
3 searching the database for the location of a key blob associated with the new  
4 migratable storage key;  
5 loading a copy of the key blob created with the non-migratable storage  
6 key; and  
7 decrypting the data.

1 17. The method as recited in claim 14, further comprising the steps of:  
2 requesting migration of new migratable signing keys;  
3 searching the database for the location of a key blob associated with a non-  
4 migratable parent of the key to be migrated;  
5 processing the migration.

1 18. In a data processing system, a method comprising the steps of:  
2 creating a migratable storage tree with a storage root key; and  
3 creating a non-migratable storage tree with the storage rootkey where the  
4 migratable storage tree and the non-migratable storage tree are identically structured  
5 with corresponding keys and authentication data.

1 19. The method as recited in claim 18, wherein the migratable storage tree and  
2 the non-migratable storage tree are created by a trusted computing module  
3 in accordance with Trusted Computing Platform Alliance.

1 20. The method as recited in claim 19, wherein the migratable storage tree  
2 comprises migratable keys and a user key, wherein the non-migratable storage tree  
3 comprises non-migratable keys and a user key.

1 21. The method recited in claim 18, wherein the migratable storage tree  
2 comprises migratable keys and encrypted user data wherein the non-migratable  
3 storage tree comprises non-migratable keys and encrypted user data .

1 22. The method as recited in claim 18, wherein the non-migratable storage  
2 tree will include non-migratable storage keys corresponding to each migratable  
3 storage key in the migratable storage tree.

1 23. The method as recited in claim 18, wherein the non-migratable storage tree  
2 will include non-migratable storage keys corresponding to a subset of the migratable  
3 storage keys in the migratable storage tree.

1 24. The method as recited in claim 18, wherein use authorization in the non-  
2 migratable storage tree will be identical to use authorization in the migratable storage  
3 tree.

1 25. The method as recited in claim 18, wherein use authorization in the non-  
2 migratable storage tree can be deduced from user authorization in the migratable  
3 storage tree with additional data.

1 26. The method as recited in claim 25, wherein the use authorization in the non-  
2 migratable storage tree is obtained by hashing the concatenation of the user  
3 authorization in the migratable storage tree with a fixed string.